Zbierka súdnych rozhodnutí

NÁVRHY GENERÁLNEHO ADVOKÁTA
MANUEL CAMPOS SÁNCHEZ-BORDONA
prednesené 12. mája 2016 [1]

Vec C-582/14

Patrick Breyer
proti
Bundesrepublik Deutschland

[návrh na začatie prejudiciálneho konania, ktorý podal Bundesgerichtshof (Spolkový súdny dvor, Nemecko)]

„Spracovanie osobných údajov — Smernica 95/46/EHS — Článok 2 písm. a) a článok 7 písm. f) — Pojem ‚osobné údaje' — IP adresy — Uchovávanie poskytovateľom služieb elektronických médií — Vnútroštátna právna úprava, ktorá neumožňuje zohľadniť legitímny záujem prevádzkovateľa"

1. Adresu internetového protokolu (ďalej len „IP adresa") tvorí séria binárnych číslic, ktoré boli pridelené zariadeniu (počítač, tablet, smartfón), slúžia na jeho identifikáciu a umožňujú mu prístup k elektronickej komunikačnej sieti. Podmienkou na pripojenie zariadenia k internetu je použitie série číslic, ktorá bola pridelená poskytovateľom prístupu na internet. IP adresa sa zasiela serveru, na ktorom sa ukladá navštívená internetová stránka.

2. Poskytovatelia prístupu na internet (vo všeobecnosti telekomunikačné spoločnosti) prideľujú svojim zákazníkom dočasne pre každé pripojenie k internetu tzv. „dynamické IP adresy", ktoré sa pri ďalších prihláseniach zmenia. Tieto spoločnosti vedú záznamy, v ktorých sa uvádza, ktorá IP adresa bola v danom okamihu pridelená konkrétnemu zariadeniu. [2]

3. Majitelia internetových stránok navštevovaných prostredníctvom dynamických IP adries si taktiež obvykle uchovávajú záznamy, v ktorých uvádzajú, aké stránky boli navštívené, kedy a z akej IP adresy. Z technického hľadiska je možné, aby sa po odhlásení internetového pripojenia jednotlivých užívateľov tieto záznamy uchovali bez časového obmedzenia.

4. Dynamická IP adresa sama osebe nestačí na to, aby poskytovateľ služieb určil totožnosť užívateľov svojej internetovej stránky. Môže sa mu to však podariť, ak spojí dynamickú IP adresu s ďalšími údajmi, ktorými disponuje poskytovateľ prístupu na internet.

1 — Jazyk prednesu: španielčina.

2 — Článok 5 smernice Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES (Ú. v. EÚ L 105, 2006, s. 54) ukladá okrem iného povinnosť uchovávať na účely vyšetrovania, odhaľovania a stíhania závažných trestných činov „dátum a čas prihlásenia a odhlásenia zo služby internetového prístupu… spolu s dynamickou alebo statickou IP adresou, ktorú komunikácii pridelil poskytovateľ internetového prístupu, a užívateľské meno účastníka alebo registrovaného užívateľa".

5. Predmetom prejednávaného sporu je otázka, či dynamické IP adresy predstavujú osobné údaje v zmysle článku 2 písm. a) smernice 95/46/EHS [3]. Aby bolo možné na túto otázku odpovedať, je potrebné najprv zistiť, aký význam má na tieto účely okolnosť, že ďalšie údaje, ktoré sú nevyhnutné na zistenie totožnosti užívateľa, nemá k dispozícii majiteľ internetovej stránky, ale tretia osoba (konkrétne poskytovateľ služby prístupu na internet).

6. Pre Súdny dvor to predstavuje novú otázku, keďže v bode 51 rozsudku Scarlet Extended [4] Súdny dvor síce vyhlásil, že IP adresy „predstavujú chránené osobné údaje, pretože umožňujú presnú identifikáciu uvedených používateľov“, ale urobil tak v kontexte, v ktorom IP adresy získaval a identifikoval poskytovateľ prístupu na internet, [5] a nie poskytovateľ obsahu, ako to je v tomto prípade.

7. Ak by dynamické IP adresy predstavovali pre poskytovateľov internetových služieb osobné údaje, bolo by následne potrebné posúdiť, či spracovanie týchto údajov patrí do pôsobnosti smernice 95/46.

8. Je možné, že ak by aj predstavovali osobné údaje, nebude sa na ne vzťahovať ochrana vyplývajúca zo smernice 95/46, ak by napríklad účelom ich spracovania bolo trestné stíhanie začaté proti prípadným internetovým útočníkom. V takejto situácii smernicu 95/46 nie je možné použiť podľa jej článku 3 ods. 2 prvej zarážky.

9. Okrem toho je potrebné určiť, či poskytovateľ služieb, ktorý uchováva dynamické IP adresy užívateľov navštevujúcich jeho internetové stránky (v prejednávanej veci Spolková republika Nemecko), vystupuje ako orgán verejnej moci alebo skôr ako súkromná osoba.

10. Nakoniec, ak by sa uplatnila smernica 95/46, bolo by potrebné určiť, do akej miery je článok 7 písm. f) tejto smernice zlučiteľný s vnútroštátnou právnou úpravou, ktorá s cieľom odôvodniť spracúvanie osobných údajov obmedzuje rozsah jednej z podmienok stanovených v uvedenom článku.

I – Právny rámec

A – *Právo Únie*

11. Odôvodnenie 26 smernice 95/46 znie takto:

„(26) keďže zásady ochrany sa musia vzťahovať na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej osoby; keďže k určeniu, či je osoba identifikovateľná, by sa mali vziať do úvahy všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór [prevádzkovateľ – *neoficiálny preklad*], alebo ľubovoľná iná osoba na identifikáciu príslušnej osoby; keďže zásady ochrany sa nebudú vzťahovať na údaje poskytnuté anonymne, a to tak, že predmet údajov sa už nebude dať identifikovať; keďže zásady správania v zmysle článku 27 môžu byť užitočným nástrojom na poskytnutie poradenstva, pokiaľ ide o spôsoby, ako sa môžu údaje poskytovať anonymne a uchovávať vo forme, v ktorej nie je možné identifikovať predmet údajov“.

3 — Smernica Európskeho parlamentu a Rady z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 1995, s. 31; Mim. vyd. 13/015, s. 355).

4 — Rozsudok z 24. novembra 2011 (C-70/10, EU:C:2011:771, bod 51).

5 — Obdobná situácia nastala tiež v rozsudku z 19. apríla 2012, Bonnier Audio a i. (C-461/10, EU:C:2012:219, body 51 a 52).

12. Podľa článku 1 smernice 95/46:

„1. V súlade s touto smernicou členské štáty chránia základné práva a slobody fyzických osôb, a najmä ich právo na súkromie v súvislosti so spracovaním osobných údajov.

2. Členské štáty neobmedzujú, ani nebránia voľnému toku osobných údajov medzi členskými štátmi z dôvodov spojených s ochranou poskytnutou podľa odseku 1.“

13. Podľa článku 2 smernice 95/46:

„Na účely tejto smernice:

a) ‚osobné údaje‘ znamenajú akúkoľvek informáciu, ktorá sa týka identifikovanej alebo identifikovateľnej fyzickej osoby (‚údajového subjektu‘); identifikovateľná osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo najmä pomocou overenia identifikačného čísla alebo jedného alebo viacerých faktorov špecifických pre jeho fyzickú, fyziologickú, duševnú, hospodársku, kultúrnu alebo sociálnu identitu;

b) ‚spracovanie osobných údajov‘ (‚spracovanie‘) znamená akúkoľvek operáciu alebo komplex operácií, ktorá sa vykonáva na osobných údajoch, či už automatickými prostriedkami, alebo nie, ako je zber, zaznamenávanie, organizácia, uskladnenie, úprava alebo nahradenie, vyhľadávanie, nahliadnutie, používanie, odhalenie prenosom, šírenie alebo sprístupnenie iným spôsobom, upravenie alebo kombinácia, blokovanie, vymazanie alebo zničenie;

…

d) ‚kontrolór [prevádzkovateľ – *neoficiálny preklad*]‘ znamená fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán, ktorý sám, alebo v spojení s inými, určí účely a prostriedky spracovania osobných údajov; tam, kde sú účely a prostriedky spracovania stanovené vnútroštátnymi zákonmi a nariadeniami, alebo zákonmi a nariadeniami spoločenstva, ten, kto spracovanie riadi, alebo konkrétne kritériá pre jeho menovanie, môžu byť navrhnuté na základe vnútroštátneho práva alebo práva spoločenstva;

…

f) ‚tretia strana‘ znamená akúkoľvek fyzickú alebo právnickú osobu, štátny orgán, agentúru alebo akýkoľvek iný orgán, ako údajový subjekt, ten, kto spracovanie riadi, spracovateľ a osoby, ktoré sú na základe priameho poverenia kontrolóra [prevádzkovateľa – *neoficiálny preklad*] alebo spracovateľom poverené spracovať údaje;

…“

14. Článok 3 smernice 95/46 s názvom „Rozsah“ stanovuje:

„1. Táto smernica sa uplatňuje na spracovanie osobných údajov vcelku alebo čiastočných údajov, automatickými prostriedkami, a na spracovanie osobných údajov inými, ako automatickými prostriedkami, ktoré tvoria časť registračného systému alebo určených pre to, aby tvorili časť registračného systému.

2. Táto smernica sa neuplatňuje na spracovanie osobných údajov:

— v priebehu činností, ktoré sú mimo rozsahu zákona spoločenstva, ako sú tie, ktoré sú uvedené v hlave V a VI Zmluvy o Európskej únii a v žiadnom prípade sa neuplatňujú na operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane hospodárskej prosperity štátu, keď sa operácia spracovania týka záležitostí bezpečnosti štátu) a činností štátu v oblastiach trestného zákona;

…“

15. Prvým ustanovením kapitoly II smernice 95/46, ktorej predmetom sú „Všeobecné nariadenia týkajúce sa zákonnosti spracovania osobných údajov“, je článok 5, podľa ktorého „členské štáty stanovia, v rámci ustanovení tejto kapitoly, presnejšie podmienky zákonnosti spracovania osobných údajov“.

16. V zmysle článku 6 smernice 95/46:

„1. Členské štáty zabezpečia, že osobné údaje musia byť:

a) spracované spravodlivo a zákonne;

b) zhromaždené na špecifikované, explicitné a zákonné účely a nebudú sa ďalej spracovávať spôsobmi, ktoré nie sú zlučiteľné s týmito účelmi. Ďalšie spracovanie údajov pre historické, štatistické alebo vedecké účely sa nepovažuje za nezlučiteľné, pod podmienkou, že členské štáty zabezpečia primerané bezpečnostné opatrenia;

c) adekvátne, relevantné a nie neprimerané vo vzťahu k účelom, pre ktoré sú zhromažďované a/alebo ďalej spracované;

d) presné a tam, kde je to nevyhnutné, udržiavané aktuálne; musí sa vykonať každé primerané opatrenie, aby sa zaistilo, že údaje, ktoré sú nepresné alebo neúplné, so zreteľom na účely, pre ktoré boli zhromažďované, alebo pre ktoré sú ďalej spracovávané sa vymažú alebo skorigujú;

e) udržiavané vo forme, ktorá umožňuje identifikáciu osôb pracujúcich s údajmi počas obdobia, ktoré je nevyhnutné na účely, pre ktoré boli údaje zhromažďované, alebo pre ktoré sú ďalej spracovávané. Členské štáty stanovia primerané bezpečnostné opatrenia pre osobné údaje uložené na dlhšie obdobia pre historické, štatistické alebo vedecké použitie.

2. Úlohou kontrolóra [prevádzkovateľa – *neoficiálny preklad*] je zaistiť, aby sa vyhovelo odseku 1.“

17. V článku 7 smernice 95/46 sa stanovuje:

„Členské štáty zabezpečia, aby bolo možné osobné údaje spracovať, iba ak:

a) osoba pracujúca s údajmi poskytla svoj súhlas jednoznačne; alebo

b) spracovanie je nevyhnutné pre výkon zmluvy, ktorej osoba pracujúca s údajmi je zainteresovanou stranou, alebo aby sa vykonali opatrenia na požiadanie osoby pracujúcej s údajmi pred uzatvorením zmluvy; alebo

c) spracovanie je nevyhnutné na vyhovenie právnemu záväzku, ktorého subjektom je kontrolór [prevádzkovateľ – *neoficiálny preklad*], alebo

d) spracovanie je nevyhnutné, aby sa ochránili životné záujmy osoby pracujúcej s údajmi; alebo

e) spracovanie je nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme alebo v uplatňovaní oficiálneho poverenia zvereného kontrolórovi [prevádzkovateľovi – *neoficiálny preklad*] alebo tretej strane, ktorej sa údaje odhalia; alebo

f) spracovanie je nevyhnutné pre účely legitímnych záujmov, ktoré plní kontrolór [prevádzkovateľ – *neoficiálny preklad*], alebo tretia strana alebo strany, ktorým sú údaje odhalené, s výnimkou, ak takéto záujmy sú prevýšené záujmami týkajúcimi sa základných práv a slobôd osoby pracujúcej s údajmi, ktoré potrebujú ochranu podľa článku 1 ods. 1.“

18. V zmysle znenia článku 13 smernice 95/46:

„1. Členské štáty môžu prijať legislatívne opatrenia na obmedzenie rozsahu povinností a práv uvedených v článkoch 6 ods. 1, v článku 10 a 11 ods. 1, v článkoch 12 a 21, keď takéto obmedzenie vytvára nevyhnutné opatrenia na zabezpečenie údajov o:

a) štátnej bezpečnosti;

b) obrane;

c) verejnej bezpečnosti;

d) prevencii, vyšetrovaní, pátraní a trestnom konaní alebo porušení etiky pre predpísané profesie;

e) dôležitom hospodárskom alebo finančnom záujme členského štátu alebo Európskej únie, vrátane peňažných, rozpočtových a daňových záležitostí;

f) monitorovaní, inšpekcii alebo regulačnej funkcii spojenej aj s výkonom oficiálneho orgánu v prípadoch uvedených v písmenách c), d) a e);

g) ochrane osoby pracujúcej s údajmi alebo práv a slobôd ostatných.

…“

B – *Vnútroštátne právo*

19. § 12 Telemediengesetz (zákon o mediálnych službách, ďalej len „TMG“) [6] stanovuje:

„1. Poskytovateľ služieb je oprávnený zhromažďovať a spracúvať osobné údaje na účely sprístupnenia elektronických médií len v rozsahu, v akom to povoľuje tento zákon alebo iný právny predpis vzťahujúci sa výslovne na elektronické médiá alebo v akom na to dal užívateľ súhlas.

2. Poskytovateľ služieb je oprávnený osobné údaje na účely sprístupnenia elektronických médií spracúvať na iné účely len v rozsahu, v akom to povoľuje tento zákon alebo iný právny predpis vzťahujúci sa výslovne na elektronické médiá alebo v akom na to dal užívateľ súhlas.

3. Pokiaľ nie je stanovené inak, uplatňujú sa príslušné predpisy o ochrane osobných údajov aj v prípade, že údaje nie sú spracovávané automaticky.“

6 — Zákon z 26. januára 2007 (BGBl 2007 I, s. 179).

20. Podľa § 15 TMG:

„1. Poskytovateľ služieb je oprávnený zhromažďovať a spracúvať osobné údaje užívateľa len v rozsahu nevyhnutnom na umožnenie a zúčtovanie využitia elektronického média (údaje o využívaní). Údajmi o využívaní sú predovšetkým:

1. informácie na identifikáciu užívateľa;

2. údaje o začiatku a konci, ako aj o rozsahu jednotlivého využívania;

3. údaje o elektronických médiách využitých užívateľom.

2. Poskytovateľ služieb je oprávnený zlúčiť údaje užívateľa o využívaní týkajúce sa využitia rôznych elektronických médií len v rozsahu nevyhnutnom na zúčtovanie užívateľa.

…

4. Poskytovateľ služieb je oprávnený údaje o využívaní spracúvať aj po skončení používateľských operácií len v rozsahu nevyhnutnom na účely zúčtovania užívateľa (zúčtovacie údaje). Poskytovateľ služieb je oprávnený údaje uchovávať na účely splnenia zákonných dôb, dôb vyplývajúcich zo stanov, alebo zmluvných dôb. …“

21. V súlade s § 3 ods. 1 Bundesdatenschutzgesetz (spolkový zákon o ochrane osobných údajov, ďalej len „BDSG“)[7] „osobnými údajmi sú údaje týkajúce sa osobných alebo materiálnych podmienok identifikovanej alebo identifikovateľnej fyzickej osoby (dotknutej osoby). …“.

II – Skutkové okolnosti

22. Pán Patrick Breyer podal proti Spolkovej republike Nemecko žalobu na zdržanie sa konania vo veci uchovávania IP adries.

23. Viaceré štátne orgány Spolkovej republiky Nemecko prevádzkujú verejne prístupné internetové portály, na ktorých poskytujú aktuálne informácie. S cieľom zabrániť útokom a umožniť stíhanie útočníkov sú všetky prístupy zaznamenávané v hromadných dátových súboroch. V nich je, aj po skončení operácie, uchovávaný každý názov otváraného súboru resp. stránky, pojmy uvedené vo vyhľadávacom okne, čas vyhľadávania, množstvo prenášaných dát, hlásenie o úspešnosti vyhľadávania a IP adresa pristupujúceho počítača.

24. Pán Breyer, ktorý niektoré z uvedených stránok navštívil, svojou žalobou žiada, aby bolo Spolkovej republike Nemecko nariadené zdržať sa uchovávania IP adresy pristupujúceho hostiteľského systému žalobcu, z ktorého sú konzultované internetové stránky, alebo prenechania takéhoto uchovávania tretej osobe, pokiaľ uloženie nie je nevyhnutné na obnovenie dostupnosti elektronického média v prípade poruchy.

25. Žalobu, ktorú podal pán Breyer, súd prvého stupňa zamietol. Odvolaniu, ktoré žalobca podal, bolo však sčasti vyhovené, a Spolkovej republike Nemecko bolo nariadené zdržať sa po skončení operácie poskytnutia prístupu uchovávania údajov. Toto zdržanie sa bolo nariadené iba pre prípad, že žalobca počas operácie poskytnutia prístupu špecifikuje svoje osobné údaje, aj vo forme e-mailu, a pokiaľ uchovávanie nie je nevyhnutné na obnovenie funkčnosti elektronického média.

7 — Zákon z 20. decembra 1990 (BGBl 1990 I, s. 2954).

III – Položená otázka

26. Po tom, čo obaja účastníci konania podali opravný prostriedok „Revision“, šiesty senát Bundesgerichtshof (Spolkový súdny dvor, Nemecko) položil tieto prejudiciálne otázky, ktoré boli doručené 17. decembra 2014:

„1. Má sa článok 2 písm. a) smernice 95/46/EHS… vykladať v tom zmysle, že adresa internetového protokolu (ďalej len ‚IP adresa‘), ktorú poskytovateľ služieb uchováva v súvislosti s prístupom na internetovú stránku, je pre neho osobným údajom už vtedy, keď tretia osoba (tu poskytovateľ prístupu) disponuje ďalšími informáciami potrebnými na identifikáciu dotknutej osoby?

2. Odporuje článok 7 písm. f) smernice 95/46 vnútroštátnemu právnemu predpisu, podľa ktorého poskytovateľ služieb môže získavať a spracúvať osobné údaje užívateľa bez jeho súhlasu len v rozsahu nevyhnutnom na umožnenie a zúčtovanie konkrétneho použitia elektronického média príslušným užívateľom a podľa ktorého účel zabezpečenia celkovej funkčnosti elektronického média nemôže odôvodniť spracúvanie po skončení jednotlivých používateľských operácií?“

27. Ako vyplýva z vysvetlenia, ktoré poskytol vnútroštátny súd, žalobca mohol v súlade s nemeckým právom požadovať zdržanie sa uchovávania IP adries, ak by pri ich uchovávaní išlo v zmysle právnych predpisov o ochrane osobných údajov o zásah do základných osobnostných práv žalobcu, konkrétne do práva na „informačné sebaurčenie“ [§ 1004 ods. 1 a § 823 ods. 1 Bürgerliches Gesetzbuch (Občiansky zákonník) v spojení s článkami 1 a 2 Grundgesetz (Základný zákon)].

28. Tak by to bolo v prípade, že: a) IP adresa – v každom prípade s časom prístupu na internetovú stránku – patrí medzi „osobné údaje“ v zmysle článku 2 písm. a) v spojení s odôvodnením 26 druhou vetou smernice 95/46, resp. v zmysle § 12 ods. 1 a 3 TMG v spojení s § 3 ods. 1 BDSG a b) že neexistuje oprávnený dôvod v zmysle článku 7 písm. f) smernice 95/46, resp. § 12 ods. 1 a 3, § 15 ods. 1 a 4 TMG.

29. Podľa názoru Bundesgerichtshof (Spolkový súdny dvor) je na účely výkladu vnútroštátneho právneho predpisu (§ 12 ods. 1 TMG) nevyhnutné určiť, v akom zmysle je potrebné chápať osobnú povahu údajov, na ktoré odkazuje článok 2 písm. a) smernice 95/46.

30. Ako ďalej uvádza vnútroštátny súd, vzhľadom na to, že podľa § 15 ods. 1 TMG je poskytovateľ služieb oprávnený získavať a spracúvať osobné údaje užívateľa len v rozsahu nevyhnutnom na umožnenie a zúčtovanie využitia elektronického média (údaje o využívaní),[8] výklad tohto vnútroštátneho ustanovenia závisí od spôsobu, akým sa má vykladať článok 7 písm. f) smernice 95/46.

IV – Konanie pred Súdnym dvorom. Tvrdenia účastníkov konania

31. Písomné pripomienky predložila nemecká, rakúska a portugalská vláda a Komisia. Iba posledná uvedená inštitúcia sa spolu s pánom Breyerom zúčastnila na ústnom pojednávaní, ktoré sa konalo 25. februára 2016, na ktorom sa nemecká vláda odmietla zúčastniť.

8 — Podľa Bundesgerichtshof (Spolkový súdny dvor) sú údajmi o využívaní predovšetkým informácie na identifikáciu užívateľa, údaje o začiatku a konci jednotlivého použitia, o jeho rozsahu a údaje o elektronických médiách využitých užívateľom.

A – *Tvrdenia účastníkov konania v súvislosti s prvou otázkou*

32. Podľa pána Breyera sa za osobné údaje považujú aj také údaje, pri ktorých existuje iba teoretická možnosť spojenia s inými údajmi, t. j. možnosť vychádzajúca z prípadného abstraktného nebezpečenstva, pričom nezáleží na tom, či takéto spojenie skutočne v praxi nastane. Skutočnosť, že určitý orgán môže byť relatívne neschopný určiť totožnosť osoby podľa IP adresy podľa jeho názoru neznamená, že tejto osobe nehrozí žiadne nebezpečenstvo. Okrem toho považuje za dôležitú skutočnosť, že Nemecko uchováva údaje o jeho IP adrese pre prípad, že by bolo nevyhnutné identifikovať prípadné útoky alebo začať trestné konanie, ako to umožňuje § 113 Telekommunikationsgesetz (zákon o elektronických komunikáciách) a ako k tomu v minulosti viackrát došlo.

33. Nemecká vláda sa domnieva, že odpoveď na prvú otázku by mala byť záporná. Dynamické IP adresy podľa jej názoru neodkazujú na „identifikovanú“ osobu v zmysle článku 2 písm. a) smernice 95/46. Aby bolo možné rozhodnúť, či v zmysle tohto ustanovenia informujú o „identifikovateľnej“ osobe, musí sa na základe „relatívneho“ kritéria uskutočniť prieskum *identifikovateľnosti*. Tak to podľa názoru nemeckej vlády vyplýva z odôvodnenia 26 smernice 95/46, v ktorom sa uvádza, že by sa mali vziať do úvahy iba tie prostriedky, u ktorých je „primeraná“ pravdepodobnosť, že ich využije prevádzkovateľ alebo tretia osoba na identifikáciu príslušnej osoby. Zmienené spresnenie nasvedčuje tomu, že normotvorca Únie nemal v úmysle zahrnúť do pôsobnosti smernice 95/46 situácie, v ktorých je objektívne možné, že túto identifikáciu uskutoční akákoľvek tretia osoba.

34. Nemecká vláda sa taktiež domnieva, že pojem „osobné údaje“ v zmysle článku 2 písm. a) smernice 95/46 sa má vykladať podľa cieľa sledovaného touto smernicou, ktorým je zabezpečiť dodržiavanie základných práv. Nutnosť ochrany fyzických osôb možno vnímať rôzne v závislosti od toho, kto má tieto údaje v držbe a či má alebo nemá k dispozícii prostriedky, aby mohol tieto údaje použiť na identifikáciu týchto osôb.

35. Nemecká vláda tvrdí, že pán Breyer nie je osoba identifikovateľná podľa IP adries spojených s ostatnými údajmi, ktoré uchovávajú poskytovatelia obsahu. Na tieto účely by bolo potrebné použiť údaje, ktoré majú k dispozícii poskytovatelia prístupu k internetu, ktorí ich však z dôvodu neexistencie právneho základu nemôžu sprístupniť poskytovateľom obsahu.

36. Rakúska vláda sa naopak domnieva, že odpoveď by mala byť kladná. Podľa odôvodnenia 26 smernice 95/46 k určeniu, či je osoba identifikovateľná, nie je potrebné, aby všetkými údajmi na jej identifikáciu disponoval jediný subjekt. IP adresu možno považovať za osobný údaj, ak má tretia osoba (napríklad poskytovateľ internetového pripojenia) k dispozícii prostriedky na to, aby bez väčšieho úsilia identifikovala majiteľa tejto adresy.

37. Portugalská vláda tiež uprednostňuje kladnú odpoveď a domnieva sa, že IP adresa v spojení s dátumom navštívenia stránky predstavuje osobný údaj v rozsahu, v akom môže užívateľa identifikovať iný subjekt ako ten, ktorý uložil IP adresu.

38. Komisia takisto navrhuje kladnú odpoveď na základe riešenia, ku ktorému dospel Súdny dvor vo veci Scarlet Extended [9]. Podľa názoru Komisie vzhľadom na to, že uchovávanie IP adries slúži práve na identifikáciu užívateľov v prípade počítačových útokov, je použitie ďalších údajov uchovávaných poskytovateľmi internetových služieb prostriedok, ktorý možno použiť „rozumne“ v zmysle odôvodnenia 26 smernice 95/46. Komisia zastáva názor, že cieľ, ktorý sleduje táto smernica, ako aj články 7 a 8 Charty základných práv Európskej únie (ďalej len „Charta“), sa zasadzujú v prospech širokého výkladu článku 2 písm. a) smernice 95/46.

9 — Rozsudok z 24. novembra 2011 (C-70/10, EU:C:2011:771, bod 51).

B – *Tvrdenia účastníkov konania v súvislosti s druhou otázkou*

39. Pán Breyer zastáva názor, že článok 7 písm. f) smernice 95/46 je všeobecným ustanovením, ktorého použitie si vyžaduje ďalšie spresnenie. V súlade s judikatúrou Súdneho dvora by sa preto mali posúdiť okolnosti konkrétneho prípadu s cieľom určiť, či existujú skupiny, ktoré majú oprávnený záujem v zmysle uvedeného ustanovenia, pričom na účely uplatňovania tohto článku je nielen možné, ale aj nevyhnutné, aby pre takéto skupiny existovali osobitné pravidlá. Pán Breyer je toho názoru, že v takejto situácii je príslušná vnútroštátna právna úprava zlučiteľná s článkom 7 písm. f) smernice 95/46, keďže neexistuje záujem verejného portálu uchovávať osobné údaje alebo pretože prevažuje záujem chrániť anonymitu. Podľa jeho názoru však systematické uchovávanie osobných údajov nie je v súlade so zásadami demokratickej spoločnosti a nie je nevyhnutné, ani primerané na zabezpečenie fungovania elektronických médií, čo možno jednoducho dosiahnuť bez uchovávania týchto osobných údajov, ako dokazujú internetové stránky niektorých spolkových ministerstiev.

40. Nemecká vláda tvrdí, že na druhú otázku nie je potrebné odpovedať, keďže bola položená iba pre prípad, že by sa na prvú otázku odpovedalo kladne, čomu podľa jej názoru bránia vyššie uvedené dôvody.

41. Rakúska vláda navrhuje odpovedať v tom zmysle, že smernica 95/46 vo všeobecnosti nebráni tomu, aby sa uchovávali údaje, o ktoré ide vo veci samej, ak je to nevyhnutné na zabezpečenie riadneho fungovania elektronických médií. Táto vláda sa domnieva, že z hľadiska dodržiavania povinnosti prevádzkovateľa prijať opatrenia na ochranu týchto údajov, ktorú ukladá článok 17 ods. 1 smernice 95/46, je uchovávanie IP adresy na časovo obmedzené obdobie presahujúce čas navštívenia internetovej stránky v súlade s právnymi predpismi. Boj proti počítačovým útokom možno považovať za dôvod na vykonanie analýzy údajov súvisiacich s predchádzajúcimi útokmi a zamietnutie prístupu na internetovú stránku z určitých IP adries. Otázka primeranosti uchovávania týchto údajov, akými sú údaje vo veci samej, sa z pohľadu cieľa spočívajúceho v zabezpečení riadneho fungovania elektronických služieb a s prihliadnutím na zásady uvedené v článku 6 ods. 1 smernice 95/46 musí posudzovať z prípadu na prípad.

42. Portugalská vláda tvrdí, že článok 7 písm. f) smernice 95/46 neodporuje vnútroštátnym právnym predpisom uplatňovaným vo veci samej, pretože nemecký zákonodarca už porovnal oprávnené záujmy prevádzkovateľa na jednej strane so základnými právami a slobodami subjektov, ktorých sa tieto údaje týkajú.

43. Podľa Komisie vnútroštátna právna úprava preberajúca článok 7 písm. f) smernice 95/46 musí definovať ciele spracovania osobných údajov takým spôsobom, aby boli pre príslušného jednotlivca predvídateľné. Podľa jej názoru nemecká právna úprava túto požiadavku nespĺňa, keďže § 15 ods. 1 TMG stanovuje, že uchovávanie IP adries je povolené „len v rozsahu nevyhnutnom na umožnenie… využitia elektronického média“.

44. Z tohto dôvodu Komisia navrhuje odpovedať na druhú otázku v tom zmysle, že toto ustanovenie nebráni takému výkladu vnútroštátneho právneho ustanovenia, podľa ktorého môže verejný orgán, ktorý vystupuje ako poskytovateľ služieb, získavať a spracúvať osobné údaje užívateľa bez jeho súhlasu napriek tomu, že sledovaný cieľ spočívajúci v zabezpečení riadneho celkového fungovania elektronického prostriedku nie je v tomto vnútroštátnom právnom ustanovení dostatočne jasne a presne stanovený.

V – Posúdenie

A – *Prvá otázka*

1. Vymedzenie položenej otázky

45. Zo spôsobu, akým Bundesgerichtshof (Spolkový súdny dvor) položil prvú zo svojich prejudiciálnych otázok, vyplýva, že jej účelom je zistiť, či IP adresa, z ktorej sa pristupuje na internetovú stránku, predstavuje pre verejný orgán, ktorý je majiteľom tejto stránky, osobný údaj [v zmysle článku 2 písm. a) smernice 95/46/EHS], ak má poskytovateľ internetového pripojenia k dispozícii ďalšie údaje, ktoré umožňujú identifikáciu dotknutej osoby.

46. Znenie tejto otázky je dostatočne presné na to, aby sme mohli ihneď vylúčiť existenciu ďalších všeobecnejších otázok, ktoré by sa týkali právnej povahy IP adries v súvislosti s ochranou osobných údajov.

47. Po prvé Bundesgerichtshof (Spolkový súdny dvor) odkazuje výlučne na „dynamické IP adresy“, t. j. na adresy, ktoré sú pridelené dočasne pre jednotlivé pripojenia na sieť a pri ďalších pripojeniach sa menia. Preto sú vylúčené „pevné alebo statické IP adresy“, pre ktoré je typická ich nemennosť a umožňujú trvalú identifikáciu zariadenia pripojeného na sieť.

48. Po druhé vnútroštátny súd vychádza z predpokladu, že v prejednávanej veci nie je poskytovateľ internetovej stránky schopný identifikovať podľa dynamickej IP adresy osoby, ktoré navštevujú jeho stránky, a nemá k dispozícii ďalšie údaje, ktoré by mohli v spojení s uvedenou IP adresou umožniť túto identifikáciu. Bundesgerichtshof (Spolkový súdny dvor) uvádza, že dynamická IP adresa v tejto súvislosti nepredstavuje *pre poskytovateľov internetovej stránky* osobný údaj v zmyslu článku 2 písm. a) smernice 95/46.

49. Pochybnosti vnútroštátneho súdu vychádzajú z toho, že dynamická IP adresa by pre poskytovateľov internetovej stránky mohla predstavovať osobný údaj, *ak by tretia osoba mala k dispozícii ďalšie údaje*, ktoré by v spojení s touto adresou mohli identifikovať osoby, ktoré navštevujú jeho stránky. Je však potrebné poukázať na ďalšie dôležité spresnenie, a síce to, že Bundesgerichtshof (Spolkový súdny dvor) neodkazuje na akúkoľvek tretiu osobu, ktorá by mala tieto ďalšie údaje k dispozícii, ale výlučne na poskytovateľa internetového pripojenia.

50. Okrem iného sú teda nesporné tieto hľadiská: a) či sú statické IP adresy osobnými údajmi v zmysle smernice 95/46;[10] b) či sú dynamické IP adresy vždy a za všetkých okolností osobnými údajmi v zmysle uvedenej smernice, a nakoniec c) či je nevyhnutné, aby sa dynamické IP adresy považovali za osobné údaje hneď, čo sa vyskytne tretia osoba, ktorá by bola schopná ich použiť na identifikáciu užívateľov siete.

51. Otázne teda zostáva iba určenie, či dynamická IP adresa predstavuje pre poskytovateľov internetovej služby osobný údaj, keď má komunikačná spoločnosť, ktorá poskytuje pripojenie na internet (poskytovateľ prístupu) k dispozícii ďalšie údaje, ktoré v spojení s uvedenou adresou umožňujú identifikovať osobu, ktorá navštívila internetovú stránku spravovanú prvou uvedenou osobou.

10 — Tento problém už Súdny dvor vyriešil v rozsudkoch z 24. novembra 2011, Scarlet Extended (C-70/10, EU:C:2011:771, bod 51) a z 19. apríla 2012, Bonnier Audio a i. (C-461/10, EU:C:2012:219). V bodoch 51 a 52 posledného uvedeného rozsudku dospel Súdny dvor k záveru, že oznámené „meno a adresa… používateľa internetu využívajúceho určitú adresu IP, o ktorej sa predpokladá, že z nej boli protiprávne nahraté súbory obsahujúce chránené diela…, predstavuje spracovanie osobných údajov v zmysle článku 2 prvého odseku smernice 2002/58 v spojení s článkom 2 písm. b) smernice 95/46“.

2. O veci samej

52. Otázka, ktorá vyvstáva v prejednávanej veci, sa v nemeckej právnej teórii a judikatúre stala predmetom rozsiahlych diskusií rozdelených do dvoch názorových smerov.[11] Podľa jedného z nich (ktorý sa riadi „objektívnym“ alebo „absolútnym“ kritériom) je užívateľ identifikovateľný – a z toho dôvodu predstavuje IP adresa osobný údaj, ktorý je predmetom ochrany – keď je jeho identifikácia možná na základe jednoduchého spojenia tejto dynamickej IP adresy s údajmi poskytnutými treťou osobou (napríklad poskytovateľom internetového pripojenia) bez ohľadu na možnosti a prostriedky poskytovateľa internetového pripojenia.

53. Zástancovia druhého smeru (ktorí presadzujú „relatívne kritérium“) tvrdia, že možnosť využiť na konečnú identifikáciu užívateľa pomoc tretej osoby nie je dostatočná na to, aby mohla byť dynamickej IP adrese priznaná povaha osobného údaja. Zásadný význam má totiž to, či je osoba, ktorá má k tomuto údaju prístup, spôsobilá tento údaj prostredníctvom vlastných prostriedkov použiť a takýmto spôsobom identifikovať určitú osobu.

54. Bez ohľadu na to, akým spôsobom sa vyvíja uvedený spor vo vnútroštátnom práve, sa odpoveď Súdneho dvora musí obmedziť iba na výklad oboch ustanovení smernice 95/46, na ktoré odkazuje vnútroštátny súd, ako aj účastníci konania, t. j. výklad článku 2 písm. a)[12] a odôvodnenia 26[13] tejto smernice.

55. Dynamické IP adresy poukazujú na deň a čas, keď bola z určitého počítača (alebo iného zariadenia) navštívená určitá internetová stránka, a teda odhaľujú, akým spôsobom sa správajú užívatelia internetu, čo samo osebe môže predstavovať zásah do ich práva na rešpektovanie súkromného života,[14] ktoré zaručuje článok 8 Európskeho dohovoru o ochrane ľudských práv a základných slobôd a článok 7 Charty, ktoré spoločne s článkom 8 Európskeho dohovoru predstavujú ustanovenie, v zmysle ktorého sa musí vykladať smernica 95/46.[15] Účastníci konania v skutočnosti tento predpoklad nespochybnili a ako taký ani nie je predmetom prejudiciálnej otázky.

56. Osobu, na ktorú odkazujú uvedené informácie, nemožno považovať za „identifikovateľnú fyzickú osobu“. Dátum a hodina pripojenia, ako aj číselný zdroj tohto pripojenia, nemôžu priamo ani nepriamo odhaliť fyzickú osobu, ktorá je vlastníkom zariadenia, z ktorého bola navštívená internetová stránka, ani totožnosť užívateľa, ktorý toto zariadenie používa (môže ísť o akúkoľvek fyzickú osobu).

11 — Pozri v súvislosti s týmito názorovými smermi právnej teórie napríklad SCHREIBAUER, M.: in: *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, ESSER, M., KRAMER, P., a von LEWINSKI, K. (ed.), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, 4. vyd., § 11 Telemediengesetz (4 až 10); NINK, J., POHLE, J.: „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze“, in: *Multimedia und Recht*, 9/2015, s. 563 až 567. HEIDRICH, J., WEGENER, C.: „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging“, in: *Multimedia und Recht*, 8/2015, s. 487 až 492. LEISTERER, H.: „Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr“, in: *Computer und Recht*, 10/2015, s. 665 až 670.

12 — Znenie tohto ustanovenia je uvedené v bode 13 týchto návrhov.

13 — Znenie tohto ustanovenia je uvedené v bode 11 týchto návrhov.

14 — V tomto zmysle sa vyjadril generálny advokát P. Cruz Villalón v návrhoch, ktoré predniesol vo veci Scarlet Extended (C-70/10, EU:C:2011:255, bod 76), a k takému záveru dospel aj Európsky dozorný úradník pre ochranu údajov vo svojich stanoviskách z 22. januára 2010 k prebiehajúcim rokovaniam Európskej únie o obchodnej dohode o boji proti falšovaniu (ACTA) (Ú. v. EÚ C 147, 2010, s. 1, bod 24) a z 10. mája 2010 k návrhu smernice Európskeho parlamentu a Rady o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa zrušuje rámcové rozhodnutie 2004/68/SVV (Ú. v. EÚ C 323, 2010, s. 6, bod 11).

15 — Pozri v tomto zmysle rozsudok z 20. mája 2003, Österreichischer Rundfunk (C-465/00, C-138/01 a C-139/01, EU:C:2003:294, bod 68), ako aj návrhy, ktoré predniesla generálna advokátka J. Kokott vo veci Promusicae (C-275/06, EU:C:2007:454, bod 51 a nasl.).

57. Dynamická IP adresa však môže – buď sama osebe, alebo v spojení s ďalšími údajmi – pomôcť určiť totožnosť vlastníka zariadenia použitého na prístup k určitej internetovej stránke, a preto ju možno považovať za údaj týkajúci sa „identifikovateľnej osoby“.[16]

58. Podľa Bundesgerichtshof (Spolkový súdny dvor) dynamická IP adresa sama osebe nestačí na identifikáciu užívateľa, ktorý prostredníctvom nej otvoril internetovú stránku. Naopak, ak by poskytovateľ internetových služieb mohol prostredníctvom dynamickej IP adresy identifikovať užívateľa, išlo by bezpochyby o osobný údaj v zmysle smernice 95/46. Význam prejudiciálnej otázky je však zrejme iný, pretože z nej vyplýva, že poskytovatelia internetových služieb, o ktorých ide v spore vo veci samej, nedokážu identifikovať užívateľa výlučne na základe dynamickej IP adresy.

59. Všetci účastníci konania sa zhodujú v tom, že ak sa dynamická IP adresa spojí s ďalšími údajmi, umožní „nepriamu“ identifikáciu užívateľa. Otázkou však zostáva, či okolnosť, že môžu prípadne existovať takéto ďalšie údaje, ktoré možno spojiť s dynamickou IP adresou, môže byť sama osebe dôvodom na to, že táto adresa sa bude považovať za osobný údaj v zmysle smernice. Je teda potrebné určiť, či na tieto účely stačí, aby existovala iba abstraktná možnosť, že tieto údaje sú známe, alebo či je naopak nutné, aby tieto údaje mala k dispozícii buď osoba, ktorá dynamickú IP adresu pozná, alebo tretia osoba.

60. Účastníci konania sa vo svojich pripomienkach zamerali na výklad odôvodnenia 26 smernice 95/46, v ktorého znení upozorňujú na výraz „prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór [prevádzkovateľ – *neoficiálny preklad*], alebo ľubovoľná iná osoba na identifikáciu príslušnej osoby“. Otázka vnútroštátneho súdu sa netýka ďalších údajov, ktoré majú k dispozícii poskytovatelia služby, o ktorých ide v konaní vo veci samej. Neodkazuje ani na akúkoľvek tretiu osobu, ktorá by mohla mať k dispozícii tieto ďalšie údaje (ktoré by v spojení s dynamickou IP adresou mohli umožniť identifikáciu užívateľa), ale na poskytovateľa internetového pripojenia.

61. V prejednávanej veci teda nie je nevyhnutné, aby Súdny dvor analyzoval všetky prostriedky, ktoré môže „rozumne“ použiť žalovaná vo veci samej, aby bolo možné dynamické IP adresy, ktoré má táto žalovaná strana k dispozícii, kvalifikovať ako osobné údaje. Keďže Bundesgerichtshof (Spolkový súdny dvor) odkazuje výlučne na ďalšie údaje, ktoré má k dispozícii tretia osoba, možno konštatovať, že: a) žalovaná nemá k dispozícii ďalšie vlastné údaje, ktoré by jej umožnili identifikáciu užívateľa, b) alebo má tieto údaje k dispozícii, ale nie je spôsobilá ich na tento účel vo svojom postavení prevádzkovateľa v zmysle odôvodnenia 26 smernice 95/46 rozumne použiť.

62. Oba uvedené predpoklady závisia od skutkového posúdenia, ktoré prináleží výlučne vnútroštátnemu súdu. Ak by si Bundesgerichtshof (Spolkový súdny dvor) nebol istý tým, že žalovaná je spôsobilá rozumne použiť ďalšie údaje, ktoré má sama k dispozícii, Súdny dvor by mu mohol poskytnúť všeobecné kritériá na výklad výrazov „prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór [prevádzkovateľ – *neoficiálny preklad*]“. Žiadne také pochybnosti však neboli vyslovené, a preto podľa môjho názoru nie je na mieste, aby Súdny dvor pri tejto príležitosti vymedzil kritériá pre výklad, ktoré nie sú pre vnútroštátny súd nevyhnutné, a o ktoré vnútroštátny súd nežiadal.

16 — Možno predpokladať, že touto osobou je osoba, ktorá práve používa internet a otvorila príslušnú internetovú stránku. V súvislosti s uvedenou domnienkou možno teda predpokladať, že z údajov o dátume, hodine a číselnom zdroji prístupu k určitej internetovej stránke je možné zistiť, kto je vlastníkom príslušného zariadenia, a vyvodiť určitý nepriamy záver o spôsobe, aký sa správa na internetovej sieti. Výnimku by mohli predstavovať IP adresy pridelené zariadeniam na takých miestach, ako sú napríklad internetové kaviarne, ktorých anonymní užívatelia sú neidentifikovateľní a ktorých prevádzkové údaje nemôžu byť zdrojom žiadnych relevantných informácií o vlastníkoch týchto zariadení. To je okrem iného jediná výnimka z pravidla, podľa ktorého IP adresy predstavujú osobné údaje, ktoré pripúšťa pracovná skupina pre ochranu jednotlivcov v súvislosti so spracovaním osobných údajov zriadená smernicou 95/46 (tzv. „skupina zriadená podľa článku 29“). Jej stanovisko č. 4/2007 z 20. júna 2007 o pojme osobných údajov, WP 136, je dostupné na internetovej stránke http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

63. Podstatou položenej otázky je teda určiť, či na to, aby bolo možné dynamické IP adresy považovať za osobné údaje, je dôležitá okolnosť, že veľmi konkrétne určená tretia osoba – poskytovateľ internetového pripojenia – má k dispozícii ďalšie údaje, ktoré môžu v spojení s uvedenými adresa identifikovať užívateľa, ktorý navštívil príslušnú internetovú stránku.

64. Je znova potrebné vrátiť sa k odôvodneniu 26 smernice 95/46. Z výrazov „prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije… *ľubovoľná iná osoba*“,[17] by mohol vychádzať výklad, podľa ktorého na to, aby dynamická IP adresa mohla byť sama osebe považovaná za osobný údaj, stačilo, aby niektorá tretia osoba mohla získať ďalšie údaje (ktoré by mohli byť spojené s dynamickou IP adresou s cieľom identifikovať určitú osobu).

65. Tento maximalistický výklad by v praxi viedol k tomu, že za osobné údaje by sa považovali informácie všetkého druhu, aj keby samy osebe neboli dostatočné na to, aby umožnili identifikáciu užívateľa. Nebolo by nikdy možné s absolútnou istotou vylúčiť, že neexistuje žiadna tretia osoba, ktorá má k dispozícii ďalšie údaje, ktoré by sa mohli spojiť s uvedenými informáciami, a tak viesť k odhaleniu totožnosti určitej osoby.

66. Domnievam sa, že v dôsledku rozvoja technológií by prístup k čoraz sofistikovanejším nástrojom umožňujúcim získavať a spracúvať údaje mohol byť vo viac či menej blízkej budúcnosti značne uľahčený, čo možno považovať za dôvod na to, aby sa v predstihu zaviedli opatrenia na ochranu súkromia. Bolo vyvinuté úsilie, aby príklady rôznych druhov konania uvedených v rámci vymedzenia právnych kategórií, ktoré sú relevantné na účely ochrany údajov, boli vymedzené dostatočne široko a pružne s cieľom pokryť všetky situácie, ktoré si možno predstaviť.[18]

67. Táto obava – ktorú považujem inak za veľmi legitímnu – nemôže však podľa môjho názoru viesť k tomu, aby sa nebral do úvahy spôsob, akým bola vyjadrená normatívna vôľa zákonodarcu, a aby sa systematický výklad odôvodnenia 26 smernice 95/46 zúžil na „prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využijú“ *niektoré tretie osoby*.

68. Rovnako ako sa v odôvodnení 26 neodkazuje na žiadne prostriedky, ktoré by mohol použiť prevádzkovateľ (v prejednávanej veci poskytovateľ internetových služieb), ale iba na prostriedky, ktoré môže prevádzkovateľ „rozumne“ použiť, je nutné vychádzať z toho, že normotvorca odkazuje na „tretie osoby“, pri ktorých možno – *tiež rozumne* – predpokladať, že by sa na ne mohol prevádzkovateľ obrátiť s cieľom získať ďalšie údaje na identifikáciu. To nenastane vtedy, keď by kontakt s týmito tretími osobami bol veľmi nákladný z hľadiska ľudských a ekonomických zdrojov alebo prakticky neuskutočniteľný či zakázaný právnymi predpismi. V opačnom prípade, ako som už skôr uviedol, by bolo totiž v praxi nemožné jednotlivé prostriedky od seba vzájomne odlíšiť, keďže by neustále existovala možnosť, že niekde existuje tretia osoba, ktorá by – teraz alebo v budúcnosti – mohla mať k dispozícii ďalšie údaje, ktoré by mohli pomôcť identifikovať užívateľa, a to bez ohľadu na to, či by táto osoba bola pre poskytovateľov internetových služieb dostupná.

69. Už som poukázal na to, že tretia osoba, na ktorú sa odvoláva Bundesgerichtshof (Spolkový súdny dvor), je poskytovateľ internetového pripojenia. Je veľmi pravdepodobné, že na túto tretiu osobu by sa poskytovateľ služieb obrátil s cieľom získať ďalšie konkrétne údaje, ak by mal v úmysle nájsť čo najúčinnejší, najpraktickejší a najľahší spôsob, akým identifikovať užívateľa, ktorý vyvolal jeho stránku prostredníctvom dynamickej IP adresy. V žiadnom prípade nejde o hypotetickú tretiu osobu, ktorá by

17 — Kurzívou zvýraznil generálny advokát.

18 — Z tejto snahy zabezpečiť predbežnú ochranu a prevenciu vychádza tiež postoj skupiny zriadenej podľa článku 29, podľa ktorého, ako som už uviedol vyššie, je potrebné vychádzať zo zásady, že IP adresy predstavujú osobné údaje, a to s jedinou výnimkou, ktorá predstavuje situácie, keď môže poskytovateľ služby s úplnou istotou určiť, že ide o adresy neidentifikovateľných osôb, napríklad návštevníkov *internetovej kaviarne*. Pozri poznámku pod čiarou 16 *in fine*.

bola neznáma a nedostupná, ale o hlavného aktéra internetovej siete, pri ktorom je úplne isté, že má k dispozícii údaje, ktoré potrebuje poskytovateľ služieb na identifikáciu určitého užívateľa. Ako teda uvádza vnútroštátny súd, na túto konkrétnu tretiu osobu má žalovaná v konaní vo veci samej v úmysle obrátiť sa s cieľom získať ďalšie údaje, ktoré považuje za nevyhnutné.

70. Poskytovateľ internetového pripojenia je typickou treťou osobu, na ktorú odkazuje odôvodnenie 26 smernice 95/46 v tom zmysle, že možno „rozumne“ predpokladať, že sa na ňu poskytovateľ služieb v prejednávanej veci obráti. Zostáva teda zistiť, či získanie ďalších údajov, ktoré má táto tretia osoba k dispozícii, možno považovať za „rozumne“ možné alebo uskutočniteľné.

71. Nemecká vláda tvrdí, že údaje, ktoré má k dispozícii poskytovateľ internetového pripojenia, majú osobnú povahu, a preto ich tento poskytovateľ môže poskytnúť iba v súlade s právnymi predpismi upravujúcimi spracovanie týchto údajov. [19]

72. Je to nepochybne tak, keďže na získanie takýchto údajov je potrebné dodržiavať právne predpisy uplatňované na osobné údaje. Takéto údaje možno získať „rozumne“ iba za predpokladu, že boli splnené podmienky stanovené pre prístup k tomuto druhu údajov, pričom prvá z podmienok sa týka zákonnej možnosti uchovávania údajov a ich prenosu tretím osobám. Je pravda, že poskytovateľ internetového pripojenia je oprávnený odmietnuť poskytovanie požadovaných údajov, ale môže nastať aj opačný prípad. Možnosť prenosu údajov, ktorá je úplne „rozumná“, je dôvodom na to, aby sa podľa odôvodnenia 26 smernice 95/46 predpokladalo, že dynamická IP adresa predstavuje pre poskytovateľa internetových služieb osobný údaj.

73. Táto možnosť je v *rámci práva* uskutočniteľná, a teda „rozumná“. Rozumné prostriedky prístupu, na ktoré odkazuje smernica 95/46, musia byť v zásade v súlade s právnymi predpismi. [20] Ako uvádza nemecká vláda, je logické, že z takého predpokladu vychádza vnútroštátny súd. [21] Tým sa významne zužuje okruh možností, ktorými možno z právneho hľadiska získať prístup k údajom, keďže musí ísť výlučne o možnosti, ktoré sú povolené. Pokiaľ však takéto možnosti existujú, bez ohľadu na to, aká obmedzená môže byť ich uplatniteľnosť v praxi, predstavujú „rozumný prostriedok“ v zmysle smernice 95/46.

74. Preto sa domnievam, že na prvú z prejudiciálnych otázok v podobe, v akej ju predložil Bundesgerichtshof (Spolkový súdny dvor), je potrebné odpovedať kladne. Dynamická IP adresa musí pre poskytovateľa internetových služieb predstavovať osobný údaj, a to vzhľadom na existenciu tretej osoby (poskytovateľa internetového pripojenia), na ktorú sa prvá uvedená osoba môže rozumne obrátiť s cieľom získať ďalšie údaje, ktoré v spojení s uvedenou adresou môžu umožniť identifikáciu určitého užívateľa.

75. Myslím si, že v prospech môjho návrhu hovorí situácia, ku ktorej by viedlo opačné riešenie. Ak by dynamické IP adresy nepredstavovali pre poskytovateľov internetových služieb osobný údaj, tento poskytovateľ by bol oprávnený uchovávať tieto adresy neobmedzene a kedykoľvek požiadať poskytovateľov internetového pripojenia o ďalšie údaje, aby ich spojil s uvedenou adresou a identifikoval tak určitého užívateľa. Ako pripúšťa nemecká vláda, [22] pokiaľ ide o uplatnenie právnych predpisov týkajúcich sa ochrany údajov, dynamická IP adresa by sa za takýchto okolností stala osobným údajom hneď po tom, ako by táto vláda už mala k dispozícii ďalšie údaje potrebné na identifikáciu určitého užívateľa.

19 — Body 40 a 45 písomných pripomienok nemeckej vlády.

20 — Za týchto okolností nie je podstatné, či prístup k osobným údajom je *de facto* uskutočniteľný porušením právnych predpisov upravujúcich ochranu údajov.

21 — Body 47 a 48 písomných pripomienok nemeckej vlády.

22 — Bod 36 písomných pripomienok nemeckej vlády.

76. Išlo by teda o údaj, ktorého uchovávanie by bolo prípustné iba vtedy, ak by doteraz nebol považovaný za údaj, ktorý by pre poskytovateľa služieb predstavoval osobný údaj. To, či sa bude dynamická IP adresa z právneho hľadiska považovať za osobný údaj, by teda výlučne záviselo od toho, či sa posledná uvedená osoba niekedy v budúcnosti rozhodne spojiť túto adresu s ďalšími údajmi, ktoré bude musieť získať od tretej osoby, a použiť ich na identifikáciu určitého užívateľa. Podľa môjho názoru je však v zmysle smernice 95/46 rozhodujúca možnosť – a to rozumná možnosť – že existuje „dostupná" tretia osoba, ktorá má k dispozícii prostriedky nevyhnutné na identifikáciu určitej osoby, a nie skutočné naplnenie tejto možnosti nadviazaním kontaktu s uvedenou treťou osobou.

77. Bolo by dokonca možné prikloniť sa aj k názoru nemeckej vlády, podľa ktorého sa dynamická IP adresa stáva osobným údajom hneď po tom, ako ju získa poskytovateľ internetového pripojenia. V takom prípade by bolo nutné pripustiť i to, že v súvislosti s dobou stanovenou na uchovávanie IP adresy môže nastať situácia, keď by sa táto kvalifikácia uskutočnila so spätnou účinnosťou a prípadne i situácia, keď by táto kvalifikácia mohla byť považovaná za neplatnú, ak by bola prekročená doba, počas ktorej táto adresa mohla byť uchovávaná, ak by bola od začiatku považovaná za osobný údaj. Taká situácia by viedla k výsledku, ktorý je v rozpore s duchom právnych predpisov týkajúcich sa ochrany osobných údajov. Dôvod, na základe ktorého sa tieto údaje majú uchovávať iba dočasne, by stratil význam v dôsledku prípadných prieťahov spojených s uznaním vlastnosti, ktorá je v samotnej povahe týchto údajov už od začiatku, a to ich schopnosť pôsobiť – buď samy osebe alebo v spojení s ďalšími údajmi – ako nástroj identifikácie určitej fyzickej osoby. Aj z tohto čisto praktického dôvodu je rozumnejšie, aby bola uvedená povaha týmto údajom priznaná už od začiatku.

78. Týmto som dospel k prvému záveru, a to že článok 2 písm. a) smernice 95/46 sa má vykladať v tom zmysle, že IP adresa, ktorú poskytovateľ služieb uchováva v súvislosti s prístupom na internetovú stránku, je pre neho osobným údajom už vtedy, keď poskytovateľ internetového pripojenia disponuje ďalšími informáciami potrebnými na identifikáciu dotknutej osoby.

B – *Druhá otázka*

79. Druhou zo svojich prejudiciálnych otázok sa Bundesgerichtshof (Spolkový súdny dvor) snaží zistiť, či článok 7 písm. f) smernice 95/46 odporuje vnútroštátnemu právnemu predpisu, podľa ktorého sa osobné údaje užívateľa môžu získať a spracúvať bez jeho súhlasu len v rozsahu nevyhnutnom na umožnenie a zúčtovanie konkrétneho použitia elektronického média príslušným užívateľom a podľa ktorého účel zabezpečenia celkovej funkčnosti elektronického média nemôže odôvodniť spracúvanie po skončení jednotlivých používateľských operácií.

80. Skôr, ako na túto otázku odpoviem, musím spresniť informácie, ktoré poskytol Bundesgerichtshof (Spolkový súdny dvor), podľa ktorého sú sporné údaje uchovávané s cieľom zabezpečiť riadne fungovanie internetových stránok, o ktoré ide vo veci samej, a v prípade potreby umožniť trestné stíhanie počítačových útokov, ktorým môžu tieto stránky čeliť.

81. Najprv je teda potrebné položiť si otázku, či spracovanie IP adries, ktoré sú predmetom návrhu na začatie prejudiciálneho konania, patrí do pôsobnosti výnimky, ktorá je stanovená v článku 3 ods. 2 prvej zarážke smernice 95/46. [23]

23 — Do pôsobnosti smernice 95/46 nepatria „operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu… a *činností štátu v oblastiach trestného zákona*" (kurzívou zvýraznil generálny advokát).

1. O uplatniteľnosti smernice 95/46 na spracovanie sporných údajov

82. Spolková republika Nemecko, ako sa zdá, vystupuje v konaní vo veci samej výlučne v postavení poskytovateľa internetových služieb, t. j. ako jednotlivec (a preto *sine imperio*). Znamená to teda, že spracovanie údajov, ktoré sú predmetom tohto sporu, nie je v zásade vylúčené z pôsobnosti smernice 95/46.

83. Ako rozhodol Súdny dvor v rozsudku Lindqvist,[24] činnosti uvedené v článku 3 ods. 2 smernice 95/46 „sú v každom prípade činnosti štátu a štátnych orgánov a nepatria do oblasti činností jednotlivcov“.[25] V rozsahu, v akom je za spracovanie sporných údajov zodpovedná osoba, ktorá aj napriek postaveniu verejného orgánu vystupuje v skutočnosti ako súkromnoprávny subjekt, je uplatniteľná smernica 95/46.

84. Vnútroštátny súd zdôrazňuje, že hlavným cieľom, ktorý nemecký správny orgán sleduje pri uchovávaní dynamických IP adries, je „zabezpečenie zachovania bezpečnosti a funkčnosti elektronického média“; uvedené platí predovšetkým na rozpoznanie a obranu proti častým útokom typu „Denial-of-Service“, pri ktorých je telekomunikačná infraštruktúra paralyzovaná cieleným a koordinovaným prúdom veľkého množstva dopytov od jednotlivých internetových serverov.[26] Uchovávanie dynamických IP adries na tento účel je typické pre všetkých majiteľov významnejších internetových stránok a nesúvisí priamo ani nepriamo s výkonom verejnej moci, takže by nemali existovať žiadne prekážky, ktoré by bránili jeho zahrnutiu do pôsobnosti smernice 95/46.

85. Bundesgerichtshof (Spolkový súdny dvor) však upozorňuje na okolnosť, že ďalším z dôvodov, prečo poskytovatelia služieb, o ktorých ide vo veci samej, uchovávajú dynamické IP adresy, je možnosť začať v prípade potreby trestné konanie proti prípadným páchateľom počítačových útokov. Stačí tento cieľ na to, aby bolo spracovanie týchto údajov vylúčené z pôsobnosti smernice 95/46?

86. Domnievam sa, že ak sa „trestné stíhanie“ bude chápať v tom zmysle, že poskytovatelia služieb žalovaní v konaní vo veci samej vykonávajú *ius puniendi* v rámci činnosti štátu, bude daná činnosť predstavovať „činnosti štátu v oblastiach trestného zákona“, ktoré patria medzi výnimky stanovené v článku 3 ods. 2 prvej zarážke smernice 95/46.

87. V súlade s judikatúrou, ktorú Súdny dvor zaviedol vo veci Huber,[27] by za takýchto okolností spracovanie osobných údajov, ktoré uskutočňujú poskytovatelia služieb s cieľom zabezpečiť bezpečnosť a technickú funkčnosť elektronického média, patrilo do pôsobnosti smernice 95/46, zatiaľ čo spracovanie údajov zameraných na činnosti štátu v oblastiach trestného práva je z pôsobnosti tejto smernice vylúčené.

88. Rovnako ako v prípade, že Spolková republika Nemecko by neviedla trestné stíhanie ako také, keďže by v postavení samotného poskytovateľa služieb nemala takúto právomoc, ale by iba predávala tak, ako každý iný jednotlivec, sporné IP adresy štátnemu represívnemu orgánu, by cieľom spracovania dynamických IP adries bola činnosť, ktorá je vylúčená z pôsobnosti smernice 95/46.

24 — Rozsudok zo 6. novembra 2003 (C-101/01, EU:C:2003:596, bod 43).

25 — Pozri v tom istom zmysle rozsudok zo 16. decembra 2008, Satakunnan Markkinapörssi a Satamedia (C-73/07, EU:C:2008:727, bod 41).

26 — Bod 36 návrhu na začatie prejudiciálneho konania.

27 — Rozsudok zo 16. decembra 2008 (C-524/06, EU:C:2008:724, bod 45).

89. Tento záver vyplýva z judikatúry ustálenej vo veci Parlament/Rada a Komisia,[28] v ktorej Súdny dvor uviedol, že z dôvodu, že určité osobné údaje „zhromaždili súkromní podnikatelia na komerčné účely a že títo podnikatelia zabezpečujú ich prenos do tretej krajiny“, neznamená, že „dotknutý prenos nepatrí do pôsobnosti“ článku 3 ods. 2 prvej zarážky smernice 95/46, pokiaľ sa uskutočňuje s cieľom súvisiacim s činnosťami štátu v oblasti trestného práva, keďže v takom prípade tento prenos „patrí do rámca vytvoreného orgánmi verejnej moci na účely verejnej bezpečnosti“.[29]

90. Naopak, ako si myslím, ak sa podľa rozhodnutia vnútroštátneho súdu „trestné stíhanie“ musí chápať v tom zmysle, že predstavuje konanie jednotlivca ako subjektu oprávneného na to, aby prostredníctvom príslušného konania začal výkon *ius puniendi*, ktorý prináleží štátu, nemožno tvrdiť, že predmetom spracovania IP adries sú činnosti štátu v oblasti trestného práva, ktoré sú vylúčené z pôsobnosti smernice 95/46.

91. Uchovávanie a ukladanie takýchto údajov totiž predstavuje ďalší dôkazný prostriedok, ktorý môže majiteľ internetovej stránky použiť na to, aby požiadal štát o stíhanie určitého protiprávneho konania na návrh účastníka konania. V konečnom dôsledku teda ide o nástroj, ktorým možno v trestnom konaní brániť práva, ktoré konkrétnemu jednotlivcovi (v prejednávanej veci verejnému subjektu, ktorý vystupuje v súkromnoprávnom režime) priznáva právny poriadok. Z tohto pohľadu sa nelíši od konania akéhokoľvek poskytovateľa internetových služieb, ktorý sa u štátu domáha ochrany v súlade s postupmi, ktorými možno podľa vnútroštátneho právneho poriadku viesť trestné stíhanie.

92. V dôsledku toho v rozsahu, v akom nemecký správny orgán vystupuje ako poskytovateľ internetových služieb, ktorý nie je poverený výkonom verejnej moci, čo prináleží posúdiť vnútroštátnemu súdu, spadá ním uskutočnené spracovanie dynamických IP adries ako osobných údajov do pôsobnosti smernice 95/46.

2. O veci samej

93. Podľa § 15 ods. 1 TMG sa osobné údaje užívateľa môžu získavať a spracúvať len v rozsahu nevyhnutnom na umožnenie a zúčtovanie využitia elektronického média. Presnejšie, poskytovateľ služieb môže získavať a využívať tzv. „údaje o využívaní“, t. j. osobné údaje užívateľa, ktoré sú nevyhnutné na „umožnenie a zúčtovanie využitia elektronického média“. Tieto údaje musia byť po ukončení využívania služby (t. j. v okamihu, keď sa ukončí konkrétne využitie elektronického média) odstránené okrem prípadov, keď je ich uchovávanie nevyhnutné „na účely zúčtovania“, ako je stanovené v § 15 ods. 4 TMG.

94. Zdá sa, že § 15 TMG neumožňuje, aby sa údaje o využívaní zaznamenávali po ukončení pripojenia z iných dôvodov; a to ani preto, aby bolo zo všeobecného hľadiska zabezpečené „umožnenie použitia elektronického média“. Vzhľadom na to, že uvedené ustanovenie TMG uvádza, že jediným dôvodom na uchovávanie údajov môže byť zúčtovanie, mohlo by sa vykladať v tom zmysle (napriek tomu, že o jeho výklade musí s konečnou platnosťou rozhodnúť vnútroštátny súd), že vyžaduje, aby boli údaje o využívaní použité výlučne s cieľom umožniť konkrétne spojenie a po jeho ukončení odstránené.

28 — Rozsudok z 30. mája 2006 (C-317/04 a C-318/04, EU:C:2006:346, body 54 až 59).

29 — Tamže, bod 59. Uvedená vec sa týkala osobných údajov, ktorých spracovanie nebolo nevyhnutné na poskytovanie služieb, ktoré boli predmetom podnikania dotknutých súkromných subjektov (leteckých spoločností), ale museli tieto subjekty predávať orgánom Spojených štátov amerických na účely prevencie a boja proti terorizmu.

95. Spôsob, akým je spracovanie osobných údajov zaručené v článku 7 písm. f) smernice 95/46,[30] by som označil za veľkorysejší (vo vzťahu k prevádzkovateľovi) ako spôsob, ktorý vyplýva z doslovného znenia § 15 TMG. V tomto smere možno nemecké ustanovenie považovať za striktnejšie ako ustanovenie Únie, keďže v podstate nepredpokladá, že by mohol byť sledovaný iný oprávnený záujem, ako je záujem súvisiaci so zúčtovaním danej služby, takže Spolková republika Nemecko by v postavení poskytovateľa internetových služieb mohla mať oprávnený záujem na tom, aby zabezpečila riadne fungovanie internetových stránok, a to i po ukončení jednotlivých prístupov k nim.[31]

96. Judikatúra Súdneho dvora v rozsudku ASNEF a FECEMD[32] poskytuje návod, ako odpovedať na druhú prejudiciálnu otázku. Súdny dvor uviedol, že z cieľa sledovaného smernicou 95/46 „vyplýva…, že článok 7 smernice 95/46 stanovuje taxatívny zoznam prípadov, v ktorých možno spracovanie osobných údajov považovať za prípustné“.[33] Z toho vyplýva, že „členské štáty nemôžu ani pridať nové zásady týkajúce sa zákonnosti spracovania osobných údajov do článku 7 smernice 95/46, ani stanoviť dodatočné požiadavky, ktoré by menili rozsah jednej zo šiestich zásad stanovených v tomto článku“.[34]

97. § 15 TMG nedopĺňa k požiadavkám, ktorými je podľa článku 7 smernice 95/46 podmienené oprávnené spracovanie údajov, žiadnu novú požiadavku – ako to bolo vo veciach ASNEF a FECEMD –,[35] ale, ak by sa vykladal obmedzujúcim spôsobom, na ktorý poukazuje vnútroštátny súd, obmedzil by rozsah podmienky uvedenej v písmene f) uvedeného ustanovenia: kde zákonodarca odkazuje všeobecne na splnenie „legitímnych záujmov, ktoré plní kontrolór [prevádzkovateľ – *neoficiálny preklad*], alebo tretia strana alebo strany, ktorým sú údaje odhalené“, § 15 TMG stanovuje iba to, že je nevyhnutné „umožnenie a zúčtovanie [konkrétneho] využitia elektronického média“.

98. Rovnako ako vo veciach ASNEF a FECEMD,[36] aj v prejednávanej veci by vnútroštátne opatrenie – opätovne upozorňujem, že iba v prípade, že sa bude vykladať uvedeným obmedzujúcim spôsobom – zmenilo rozsah zásady uvedenej v článku 7 smernice 95/46 namiesto toho, aby ho iba spresnilo, čo je podľa článku 5 smernice 95/46 jediná možnosť, pre ktorú bola orgánom každého členského štátu priznaná istá miera voľnej úvahy.

99. Podľa tohto uvedeného ustanovenia „členské štáty stanovia, v rámci ustanovení tejto kapitoly,[37] presnejšie podmienky zákonnosti spracovania osobných údajov“. Vo veciach ASNEF a FECEMD[38] však Súdny dvor uviedol, že „členské štáty nemôžu [na základe uvedeného ustanovenia] ani zaviesť iné zásady týkajúce sa zákonnosti spracovania osobných údajov, než sú uvedené v článku 7 tejto smernice, ani meniť dodatočnými požiadavkami rozsah šiestich zásad stanovených v predmetnom článku 7“.

30 — Už citovaný v bode 17 týchto návrhov.

31 — Pozri bod 84 týchto návrhov. Majitelia internetových stránok majú samozrejme legitímny záujem na prevencii prípadov odmietnutia služby („denials-of-service“), na ktoré odkazuje vnútroštátny súd, t. j. rozsiahlych útokov, ktoré bývajú niekedy koordinovaným spôsobom namierené proti určitým internetovým stránkam s cieľom zahltiť ich a vyradiť ich z prevádzky.

32 — Rozsudok z 24. novembra 2011 (C-468/10 a C-469/10, EU:C:2011:777).

33 — Tamže, bod 30.

34 — Tamže, bod 32.

35 — V uvedenom prípade vnútroštátne právne predpisy doplnili požiadavky stanovené v článku 7 písm. f) smernice 95/46 o požiadavku, podľa ktorej museli byť spracovávané údaje uvedené vo verejne prístupných zdrojoch.

36 — Rozsudok z 24. novembra 2011 (C-468/10 a C-469/10, EU:C:2011:777).

37 — Kapitola II s názvom „Všeobecné nariadenia týkajúce sa zákonnosti spracovania osobných údajov“, ktorej súčasťou sú články 5 až 21 smernice 95/46.

38 — Rozsudok z 24. novembra 2011 (C-468/10 a C-469/10, EU:C:2011:777, bod 36).

100. § 15 TMG by v porovnaní s článkom 7 písm. f) smernice 95/46 výrazne obmedzil rozsah legitímneho záujmu, ktorým možno odôvodniť spracúvanie údajov namiesto toho, aby ho len spresnil alebo vysvetlil v medziach stanovených článkom 5 uvedenej smernice. Jeho znenie je navyše kategorické a jednoznačné, pričom nepripúšťa, aby sa ochrana a zabezpečenie všeobecného používania elektronického média stali predmetom posúdenia, ktorého cieľom by bolo zistiť, či neprevyšujú „záujmy týkajúce sa základných práv a slobôd osoby pracujúcej s údajmi, ktoré potrebujú ochranu podľa článku 1 ods. 1“ smernice 95/46, ako stanovuje článok 7 písm. f) tejto smernice.

101. V konečnom dôsledku rovnako ako vo veciach ASNEF a FECEMD [39] stanovil nemecký zákonodarca „konečný výsledok vyplývajúci z posúdenia protichodných práv a záujmov [určitých kategórií osobných údajov] bez toho, aby pripustil odlišný výsledok vychádzajúci z osobitných okolností konkrétneho prípadu“, takže „nejde už o spresnenie v zmysle… článku 5“ smernice 95/46.

102. Za týchto okolností sa domnievam, že spôsob, akým bude Bundesgerichtshof (Spolkový súdny dvor) vykladať vnútroštátne právne predpisy, musí byť v súlade so smernicou 95/46 v tom zmysle, že: a) medzi dôvody, ktorými možno odôvodniť spracúvanie tzv. „údajov o využívaní“, musí byť možné zaradiť tiež legitímny záujem poskytovateľov elektronických médií týkajúci sa ochrany ich všeobecného využívania a b) musí byť umožnené posúdiť v každom konkrétnom prípade tento záujem poskytovateľa služieb vo vzťahu k záujmu a základným právam užívateľa s cieľom určiť, ktorý z týchto záujmov si vyžaduje ochranu podľa článku 1 ods. 1 smernice 95/46. [40]

103. Podľa môjho názoru k uvedenému postupu, ktorým by sa takéto posúdenie malo uskutočniť vo veci, ktorá je predmetom návrhu na začatie prejudiciálneho konania, nie je čo dodať. Bundesgerichtshof (Spolkový súdny dvor) v tejto súvislosti nepredkladá žiadnu otázku, keďže jeho pochybnosti sa týkajú otázky, ktorá takému posúdeniu predchádza, t. j. otázky, či je takéto posúdenie možné.

104. Nakoniec považujem za zbytočné uvádzať, že vnútroštátny súd bude môcť zohľadniť zákonné ustanovenia, ktoré prípadne prijme členský štát na základe splnomocnenia podľa článku 13 ods. 1 písm. d) smernice 95/46 s cieľom obmedziť rozsah povinností stanovených v článku 6 tejto smernice, ak je to nevyhnutné na to, aby okrem iného boli tiež zabezpečené údaje „… prevencii, vyšetrovaní, pátraní a trestnom konaní…“. Ani na toto hľadisko neodkazuje vnútroštátny súd, keďže si je bezpochyby vedomý existencie oboch týchto článkov.

105. V dôsledku toho navrhujem na druhú prejudiciálnu otázku odpovedať tak, že článok 7 písm. f) smernice 95/46 odporuje vnútroštátnej právnej úprave, ktorej výklad bráni poskytovateľovi služieb v tom, aby s cieľom zabezpečiť celkovú funkčnosť elektronického média získal a spracúval osobné údaje užívateľa bez jeho súhlasu po skončení jednotlivých používateľských operácií.

VI – Návrh

106. Vzhľadom na uvedené navrhujem, aby Súdny dvor odpovedal na položené prejudiciálne otázky takto:

1. Podľa článku 2 písm. a) smernice Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov dynamická IP adresa, prostredníctvom ktorej užívateľ otvoril internetovú stránku poskytovateľa

39 — Tamže, bod 47.

40 — Právny zástupca pána Breyera na pojednávaní vylúčil, že by uchovávanie dynamických IP adries bolo nevyhnutné na to, aby bolo riadne fungovanie internetových služieb chránené pred prípadnými útokmi. Tento problém podľa môjho názoru nie je možné vyriešiť v absolútnom ponímaní, keďže sa musí naopak riešiť v každom konkrétnom prípade osobitne, a to na základe porovnania záujmu majiteľa internetovej stránky s právami a záujmami užívateľov.

elektronických médií, predstavuje pre tohto poskytovateľa „osobný údaj“ v rozsahu, v akom má poskytovateľ internetového pripojenia k dispozícii ďalšie údaje, ktoré v spojení s dynamickou IP adresou umožňujú identifikáciu užívateľa.

2. Článok 7 písm. f) smernice 95/46 sa má vykladať v tom zmysle, že účel zabezpečenia celkovej funkčnosti elektronického média sa môže v zásade považovať za legitímny záujem, ktorého splnenie odôvodňuje spracúvanie tohto osobného údaja, pričom sa musí posúdiť, či tento záujem prevyšuje záujem alebo základné práva dotknutej osoby. Vnútroštátne ustanovenie, ktoré neumožňuje zohľadniť tento legitímny záujem, je nezlučiteľné s uvedeným článkom.